

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/US04/043405

International filing date: 22 December 2004 (22.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/533,769
Filing date: 31 December 2003 (31.12.2003)

Date of receipt at the International Bureau: 28 January 2005 (28.01.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse



THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

January 12, 2005

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE.

APPLICATION NUMBER: 60/533,769

FILING DATE: *December 31, 2003*

RELATED PCT APPLICATION NUMBER: *PCT/US04/43405*



Certified By

Jon W Dudas

Under Secretary
of Commerce for Intellectual Property
and Acting Director of the
United States Patent and Trademark Office

17638 U.S. PTO
123103

PTO/SB/16 (08-03) (AW 10/2003)

Approved for use through 7/31/2006. OMB 0651-0032

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Express Mail Label No. EV351885485US

| INVENTOR(S) | | |
|---|--|---|
| Given Name (first and middle [if any]) | Family Name or Surname | Residence (City and either State or Foreign Country) |
| Dennis V. | Pollutro | Clymer, New York |
| Andrew A. | Almquist | Jamestown, New York |
| <input type="checkbox"/> Additional inventors are being named on the <u>separately numbered sheet(s) attached hereto</u> | | |
| TITLE OF THE INVENTION (500 characters max) | | |
| METHOD AND SYSTEM FOR ESTABLISHING THE IDENTITY OF AN ORIGINATOR OF COMPUTER TRANSACTIONS | | |
| CORRESPONDENCE ADDRESS | | |
| Direct all correspondence to: | | |
| <input checked="" type="checkbox"/> Insert Customer Number <u>23122</u> | | |
| OR | | |
| <input type="checkbox"/> Firm or Individual Name | | |
| Address | | |
| Address | | |
| City | State | Zip Code |
| Country | Telephone No. | Fax No. |
| ENCLOSED APPLICATION PARTS (check all that apply) | | |
| <input checked="" type="checkbox"/> Specification - Number of Pages <u>17</u> | <input type="checkbox"/> CD(s) - Number <u> </u> | |
| <input checked="" type="checkbox"/> Drawing(s) - Number of Sheets <u>5</u> | <input checked="" type="checkbox"/> Other (please specify) <u>Express Mail Certificate, Return Receipt Postcard, Fee Transmittal (2)</u> | |
| <input type="checkbox"/> Application Data Sheet (see 37 CFR 1.76) | | |
| METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT (check one) | | |
| <input checked="" type="checkbox"/> Applicant(s) claim(s) small entity status (see 37 CFR 1.27) | | |
| <input checked="" type="checkbox"/> A check or money order is enclosed to cover the filing fees. | | |
| <input checked="" type="checkbox"/> The Director is hereby authorized to charge filing fees or credit any overpayment to Deposit Account No.: <u>18-0350</u> Filing Fee Amount <u>\$80.00</u> | | |
| <input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached. | | |
| The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government. | | |
| <input checked="" type="checkbox"/> No. | | |
| <input type="checkbox"/> Yes, the name of the U.S. Government Agency and the Government Contract Number are: | | |

[Page 1 of 1]

Respectfully submitted,

SIGNATURE

Joshua L. Cohen

Date: December 31, 2003

Registration No.: (if appropriate):

38,040

TYPED or PRINTED NAME Joshua L. Cohen

TELEPHONE NUMBER (610) 407-0700

Docket Number:

SYNC-103USP

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NO SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop Provisional Patent Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

15535 U.S. PTO
60/533769
123103

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**FEE TRANSMITTAL
for FY 2004**

Effective 10/01/2003. Patent fees are subject to annual revision.

☒ Applicant claims small entity status. See 37 CFR 1.27**TOTAL AMOUNT OF PAYMENT** (\$) 80**Complete if Known**

Application Number To Be Assigned

Filing Date Herewith

First Named Inventor Dennis V. Polluto

Examiner Name To Be Assigned

Art Unit To Be Assigned

Attorney Docket No. SYNC-103USP

METHOD OF PAYMENT (check all that apply)☒ Check ☐ Credit Card ☐ Money ☐ Other ☐ None
Order☒ Deposit Account:Deposit
Account
Number

18-0350

Deposit
Account
Name

RatnerPrestia

The Director is authorized to: (check all that apply)

☐ Charge fee(s) indicated below☒ Credit any overpayments☒ Charge any additional fee(s) or any underpayment of fee(s)☐ Charge fee(s) indicated below, except for the filing fee to the above-identified deposit account.**FEE CALCULATION****1. BASIC FILING FEE**

| Large Entity | | Small Entity | | Fee Description | Fee Paid |
|--------------|----------|--------------|----------|------------------------|----------|
| Fee Code | Fee (\$) | Fee Code | Fee (\$) | | |
| 1001 | 770 | 2001 | 385 | Utility filing fee | |
| 1002 | 340 | 2002 | 170 | Design filing fee | |
| 1003 | 530 | 2003 | 265 | Plant filing fee | |
| 1004 | 770 | 2004 | 385 | Reissue filing fee | |
| 1005 | 160 | 2005 | 80 | Provisional filing fee | 80 |

SUBTOTAL (1)

(\$ 80)

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

| Total Claims | | Extra Claims | | Fee from below | | Fee Paid |
|--------------------|-------|--------------|-----|----------------|---|----------|
| | -20** | = 0 | X | | = | 0 |
| Independent Claims | | -3** | = 0 | X | = | 0 |
| Multiple Dependent | | | X | | = | 0 |

| Large Entity | | Small Entity | | Fee Description |
|--------------|----------|--------------|----------|--|
| Fee Code | Fee (\$) | Fee Code | Fee (\$) | |
| 1202 | 18 | 2202 | 9 | Claims in excess of 20 |
| 1201 | 86 | 2201 | 43 | Independent claims in excess of 3 |
| 1203 | 290 | 2203 | 145 | Multiple dependent claim, if not paid |
| 1204 | 86 | 2204 | 43 | ** Reissue independent claims over original patent |
| 1205 | 18 | 2205 | 9 | ** Reissue claims in excess of 20 and over original patent |

SUBTOTAL (2)

(\$ 0)

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)**3. ADDITIONAL FEES**

| Large Entity | | Small Entity | | Fee Description | Fee Paid |
|--------------|----------|--------------|----------|--|----------|
| Fee Code | Fee (\$) | Fee Code | Fee (\$) | | |
| 1051 | 130 | 2051 | 65 | Surcharge - late filing fee or oath | |
| 1052 | 50 | 2052 | 25 | Surcharge - late provisional filing fee or cover sheet | |
| 1053 | 130 | 1053 | 130 | Non-English specification | |
| 1812 | 2,520 | 1812 | 2,520 | For filing a request for <i>ex parte</i> reexamination | |
| 1804 | 920* | 1804 | 920* | Requesting publication of SIR prior to Examiner action | |
| 1805 | 1,840* | 1805 | 1,840* | Requesting publication of SIR after Examiner action | |
| 1251 | 110 | 2251 | 55 | Extension for reply within first month | |
| 1252 | 420 | 2252 | 210 | Extension for reply within second month | |
| 1253 | 950 | 2253 | 475 | Extension for reply within third month | |
| 1254 | 1,480 | 2254 | 740 | Extension for reply within fourth month | |
| 1255 | 2,010 | 2255 | 1,005 | Extension for reply within fifth month | |
| 1401 | 330 | 2401 | 165 | Notice of Appeal | |
| 1402 | 330 | 2402 | 165 | Filing a brief in support of an appeal | |
| 1403 | 290 | 2403 | 145 | Request for oral hearing | |
| 1451 | 1,510 | 1451 | 1,510 | Petition to institute a public use proceeding | |
| 1452 | 110 | 2452 | 55 | Petition to revive - unavoidable | |
| 1453 | 1,330 | 2453 | 665 | Petition to revive - unintentional | |
| 1501 | 1,330 | 2501 | 665 | Utility issue fee (or reissue) | |
| 1502 | 480 | 2502 | 240 | Design issue fee | |
| 1503 | 640 | 2503 | 320 | Plant issue fee | |
| 1460 | 130 | 1460 | 130 | Petitions to the Commissioner | |
| 1807 | 50 | 1807 | 50 | Processing fee under 37 CFR 1.17(q) | |
| 1806 | 180 | 1806 | 180 | Submission of Information Disclosure Stmt | |
| 8021 | 40 | 8021 | 40 | Recording each patent assignment per property (times number of properties) | |
| 1809 | 770 | 2809 | 385 | Filing a submission after final rejection (37 CFR § 1.129(a)) | |
| 1810 | 770 | 2810 | 385 | For each additional invention to be examined (37 CFR § 1.129(b)) | |
| 1801 | 770 | 2801 | 385 | Request for Continued Examination (RCE) | |
| 1802 | 900 | 1802 | 900 | Request for expedited examination of a design application | |

Other fee (specify)

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3)

(\$ 0)

SUBMITTED BY

Name (Print/Type)

Joshua L. Cohen

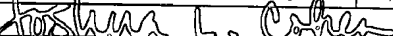
Registration No. Attorney/Agent

38,040

Telephone

(610) 407-0700

Signature



Date

December 31, 2003

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

This collection of information is required by 37 CFR 1.17 and 1.27. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

CERTIFICATE OF MAILING BY "EXPRESS MAIL" (37 CFR 1.10)

Applicant(s): Dennis V. Pollutro and Andrew A. Almquist

Docket No.

SYNC-103USP

Serial No.

Filing Date

Examiner

Group Art Unit

To Be Assigned

Herewith

Invention: METHOD AND SYSTEM FOR ESTABLISHING THE IDENTITY OF AN ORIGINATOR OF
COMPUTER TRANSACTIONS

I hereby certify that the following correspondence:

Provisional Application and its enclosures

*(Identify type of correspondence)*Is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37
CFR 1.10 in an envelope addressed to:

Mail Stop: Provisional Application,

Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

on December 31, 2003

Kathleen Libby*(Typed or Printed Name of Person Mailing Correspondence)**(Signature of Person Mailing Correspondence)*EV351885485US*("Express Mail" Mailing Label Number)***Note: Each paper must have its own certificate of mailing.**

METHOD AND SYSTEM FOR ESTABLISHING THE IDENTITY OF AN ORIGINATOR OF COMPUTER TRANSACTIONS

FIELD OF THE INVENTION

This invention relates to computer system security, and more particularly, to identifying an originator of a computer transaction.

BACKGROUND OF THE INVENTION

It is often desirable to control the accessibility of computer system resources that are accessible through networks such as LANs, WANs, and the Internet. Recently, security and access concerns have grown as malicious trespasses have increased the desirability to have improved access control. Further, the heightened state of awareness related to threats of cyber terrorism make the desire to reduce existing vulnerabilities greater than ever before.

A key to restricting access to network resources is the ability to distinguish between different users once they have been identified. Conventional methods involve creating a session identifier for a user once the user has been identified. If the client-server application is capable, the session identifier may be embedded in the application data that is sent back and forth between the client and server. One example of this is embedding a cookie in a web browser. Unfortunately, many applications were never designed to handle session identifiers and cannot practically be made to accommodate session identifiers. For such applications, present solutions relate to using the session identifier from the network address of the client. Unfortunately, network addresses are often overridden by network gateways, and as such, the reliability of this identifying information is substantially diminished.

Figure 1 is a block diagram illustration of several users (i.e., User 1, User 2, and User 3) communicating with a network through a common gateway (i.e., 192.168.1.1). Because the gateway overwrites the network addresses of the users with its own network address, the server (i.e., 192.168.1.13) sees every user coming through the gateway as having the same network address.

In configurations where it is not possible or practical to place a session identifier in the client-server application, it would be desirable to provide a method of identifying an originator of a computer transaction that overcomes at least one of the above-described deficiencies.

SUMMARY OF THE INVENTION

According to an exemplary embodiment of the present invention, a method of identifying the originator of a message transmitted between a client and a server system is provided. The method includes modifying a message to be transmitted between a client and a server system to include a session identification flag and/or a session identifier (e.g., at an end of the message). The method optionally includes one or more of the steps of re-computing a control portion of the message to reflect the inclusion of the session identification flag and the session identifier; transmitting the message between the client and the server system, and checking the transmitted message for the session identification flag; reading the session identifier of the transmitted message to determine the originator of the message; removing the session identification flag and/or the session identifier from the transmitted message; and re-computing the control portion of the message to reflect the removal of the session identification flag and/or the session identifier.

In another exemplary embodiment of the present invention, a computer system is provided. The computer system includes a

microprocessor and a computer readable medium. The computer readable medium includes computer program instructions which cause the computer system to implement the above-described method of identifying the originator of a message transmitted between a client and a server system.

In yet another exemplary embodiment of the present invention, a computer readable carrier including computer program instructions is provided. The computer program instructions cause a computer system to implement the above-described method of identifying the originator of a message transmitted between a client and a server system.

BRIEF DESCRIPTION OF THE DRAWINGS

Exemplary embodiments of the invention will be described with reference to the drawings, of which:

Figure 1 is a block diagram illustrating communications from three users to a server system through a common network gateway;

Figure 2 is a block diagram illustration of the contents of a message in a typical computer networking protocol;

Figure 3 is an illustration of the message depicted in Figure 2 modified in accordance with an exemplary embodiment of the present invention;

Figure 4 is a flow diagram illustrating a method through which a server reads messages in accordance with an exemplary embodiment of the present invention; and

Figure 5 is a flow diagram illustrating a method of identifying the originator of a message transmitted between a client and a server system in accordance with an exemplary embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

Preferred features of selected embodiments of this invention will now be described with reference to the figures. It will be appreciated that the spirit and scope of the invention is not limited to the embodiments selected for illustration. It is contemplated that any of the embodiments described hereafter can be modified within the scope of this invention.

The present invention relates to computer system security. U.S. patent application 10/423,444, filed April 25, 2003, entitled "COMPUTER SECURITY SYSTEM," also relates to computer system security, and is incorporated by reference herein in its entirety. U.S. provisional patent application filed on December 16, 2003, entitled "COMPUTER SECURITY SYSTEM" (Attorney Docket No. SYNC-101USP) also relates to computer system security, and is also incorporated by reference herein in its entirety. U.S. provisional patent application, filed concurrently herewith, entitled "METHOD AND SYSTEM FOR DELEGATING ACCESS TO COMPUTER NETWORK RESOURCES" (Attorney Docket No. SYNC-102USP) also relates to computer system security, and is incorporated by reference herein in its entirety.

Generally, an exemplary embodiment of the present invention relates to a security system that enables one, some or all users to be identified by a unique session identifier regardless of the application being used or the apparent network address of the user. Thus, users going through the same network gateway that masks their true network address can be distinguished through their unique session identifier.

In certain exemplary embodiments of the present invention, a method of modifying networking protocols is provided that is computationally simple, is compatible with existing network protocols, and is compatible with various encryption techniques. For example, the method optionally includes identifying a user and creating a corresponding session identifier. The

session identifier may be changed with each communication, may be changed at a predetermined interval, or may remain constant for the user.

If the communication/message is sent from a client to a server, the message may be modified on the client side to add a session identification flag and a session identifier at the end of the message. A control portion of the message may also be re-computed on the client side to take into account the inclusion of the session identification flag and the session identifier at the end of the message.

After transmission to the server, the message is checked on the server side for the session identification flag. If the session identification flag exists, the session identifier is read on the server side. If the session identification flag exists, the session identification flag and the session identifier are removed on the server side. The control portion of the message is then re-computed to take into account the removal of the session identification flag and the session identifier.

Of course, the process may be applied to messages from the server side to the client side. Further still, certain actions described with respect to one side (i.e., the client side or the server side) may be accomplished on the alternative side if desired.

In another embodiment, a client-server algorithm is provided in a computer readable medium that includes computer program instructions that cause servers and clients to implement the above-described method.

Through the various exemplary embodiments disclosed herein, a security system for information is provided. Additionally, methods of providing access to information, and restricting access to information, using the security system, are also disclosed. The disclosed invention is particularly suited, according to preferred embodiments, to the security of

remotely accessed network environments through a network connection though other applications are contemplated as well.

According to certain exemplary embodiments of the present invention, a message is sent to the security system from an external source (e.g., a user). A determination is made as to whether the message contains an embedded session identifier. If the message does contain an embedded session identifier, the identifier is used to determine how to process the message. The session identifier is stripped from the message and the message is repackaged into its original unmodified form and passed on appropriately. If the message does not contain an embedded session identifier, it can be rejected or processed according to the rules in place for messages without embedded session identifiers.

According to certain exemplary embodiments of the present invention used as part of a security system, the embedded session identifier allows one to reliably control the visibility of network resources to remote users of that network regardless of the application being used. For example, the network may be configured to determine a user identity from the embedded session identifier instead of the user's network address. Because of the extensive use of network address translation and network gateways, network addresses can be arbitrary. However, the security system acts as an umbrella over the remotely accessed network and allows users to be identified by a unique session identifier rather than their apparent network address.

According to an exemplary embodiment of the present invention, all connectivity to the protected network must pass through the security system though it is also contemplated that at least selected connectivity to the protected network may not pass through the security system. Once a user has been authenticated, a session identifier is created and embedded in all messages sent to and from the user according to an exemplary embodiment

of the invention. The security system then checks all incoming messages for embedded session identifiers. If the message contains an embedded session identifier, it is read. If the session identifier is valid, the message is repackaged into its original unmodified form and processed according to the rules for the user associated with that session identifier. If the session identifier is not valid, the message is dropped. If the message does not contain an embedded session identifier the message can be processed in one of two ways: it can be dropped or it can be processed according to the rules for messages without embedded session identifiers.

In certain exemplary embodiments, all communication between the user and the network is encrypted so as to hide the communications from other authenticated and non-authenticated users (including users connected via the Internet). As such, session identification modification is either done after the encryption or before the encryption. If the modification is done after the encryption, the session identification is read and the message is repackaged before it is decrypted. If the modification is done before the encryption, the message is decrypted before the session identification is read and the message is repackaged.

A timeout feature may also be provided whereby the expiration of a predetermined period of inactivity is used to determine when the session (and the session ID) should be terminated. During the user's session, the inactivity/timeout period is continually updated. The timeout period is set by resources in the network and if the user does not perform an action/interaction within the predetermined timeout period, the session is terminated by deleting it from those same resources in the network. This allows a high level of security because no meaningful information is stored on the user's computer. Further, even if someone does gain access to the user's computer, after the timeout period has expired, any information that might be stored in a cookie on the user's computer is no longer valid.

In certain embodiments of the present invention, after the user has logged in, a number of checks may take place each time the user moves within the system in order to determine what resources the user can access. For example, the security system determines the identity of the user accessing the system. The session may be validated by checking the user ID against a database of user IDs on the network. If a session ID is invalid, the session is invalid, and the user is forced to log in before accessing the system. If the session ID is valid, the system retrieves the associated user ID and continues to perform whatever actions are necessary to finish displaying the approved information.

Through various exemplary embodiments, the process of accessing a resource (e.g., an application) on a remote server begins with the user logging into the security system (e.g., logging in using single sign on software that logs the user directly into the security system). Once logged in, a session identifier is created and embedded in all communications between the user and the network. The user can run client applications that connect to applications hosted on the application server and view objects if the client applications have been pre-configured with the addresses of the application servers. If the client applications have not been pre-configured with the addresses of the application server, the user can be provided with a unique token that provides a single use link to the application server. The token either contains the information required to connect to the application server or retrieves the information required to connect to the application server. The client application then connects to the application server, and the application server then displays all objects and applications approved for the user.

The figures described herein illustrate a modification to a network protocol and may utilize common programming languages. This security system contemplates the desire to provide secure access to all remote applications, software, and content. The security system also contemplates

and provides embodiments that involve installation of the services on the remote user's device.

The security system of the present invention may be implemented in a number of mediums. For example, the system can be installed on an existing computer system/server as software. Further, the system can operate on a stand alone computer system (e.g., a security server) that is installed between another computer system (e.g., an application server) and an access point to another computer system. Further still, the system may operate from a computer readable carrier (e.g., solid state memory, optical disk, magnetic disk, radio frequency carrier wave, audio frequency carrier wave, etc.) that includes computer instructions (e.g., computer program instructions) related to the security system.

The present invention, according to the exemplary embodiments selected for illustration in the figures, relates to the modification of existing network protocols to embed a session identifier into the messages sent back and forth between a client and a server. Figure 2 is an illustration of a typical message that is sent over computer networks. The message consists of a control portion and a payload portion. The control portion contains information that allows the message to be routed to and received by the proper network location (e.g., routing information and other control information such as hardware address data). The payload contains the actual data to be communicated.

The network protocol modification consists of a client portion and a server portion. If the message is sent by a client to a server, the client portion may consist of three steps. The first step is to add a flag to the message (such as at the end of the message) that indicates that the message contains an embedded session identifier. The second step is to add the session identifier to the message (such as after the flag). Finally, the third step is to re-compute the control portion of the message to take into account the data added to the message in the first and second steps.

Figure 3 is an illustration of the message depicted in Figure 2 after modification. A flag has been added after the end of the original message. A session identifier has been added after the flag, and the control portion of the message has been altered to take into account the added flag and session identifier. For example, the control portion may include data related to the length of the data portion, or data related to a CheckSum calculation. By increasing the length of the data portion (through the inclusion of the session identifier and the flag) these values in the control portion are affected, and as such, are re-computed.

Figure 4 is an illustration of a flow diagram illustrating an exemplary method through which a server reads messages. The server desirably analyzes every message received. Step 1 is to start at the end of the message and move back by the length of the session identifier. For example, this length may be agreed upon, and as such, the server desirably knows this length. Step 2 is to move back by the length of the flag and read that data. Step 3 is to determine if the data matches the session identification flag. If the flag does not match, the message has not been modified by the protocol and one proceeds to step 4. At Step 4, the message is processed as is. If the flag does match the session identification flag the message has been modified by the protocol and one proceeds to step 5. Step 5 is to read the end of the message. Step 6 is to remove the flag and the session identifier from the end of the message. Step 7 is to re-compute the control portion of the message to take into account that the flag and session identifier have been removed from the end of the message. At Step 8, the resulting message is processed along with the session identifier.

Figure 5 is a flow diagram illustrating a method of identifying the originator of a message transmitted between a client and a server system in accordance with an exemplary embodiment of the present invention. At step 500, a message to be transmitted between a client and a server system is

modified to include a session identification flag and a session identifier at an end of the message. At step 502, a control portion of the message is re-computed to reflect the inclusion of the session identification flag and the session identifier at the end of the message. At step 504, the message is transmitted between the client and the server system. At step 506, the transmitted message is checked for the session identification flag. At step 508, the session identifier of the transmitted message is read to determine the originator of the message. At step 510, the session identification flag and the session identifier is removed from the transmitted message. At step 512, the control portion of the message is re-computed to reflect the removal of the session identification flag and the session identifier.

In certain situations, there is a chance that the data in an unmodified message will match the session identification flag. If the data in a message is random, this chance is determined by the length of the flag. If the session identification flag is 8 bits long, then the chance for a random match is 1 in 2^8 or 1 in 256. In such a case, one can calculate the chance that the erroneous session identifier will match that of an actual session identifier in use. If the session identifier is the length of an unsigned long integer, then on the typical system, this will have a length of 8 bytes. This results in about 1.8×10^{19} possible session identifiers. If such a system had as many as 10,000 active sessions, the chance that the erroneous session identifier would match that of an active session would only be 1 in 1.8×10^{14} . Thus, the chance of a message being processed erroneously would only be about 1 in 4.0×10^{16} . However, the chance that extra work is done to extract the session identifier erroneously is 1 in 256.

Thus, an efficient way to reduce the chance of erroneously processing a message and decreasing the amount of work done is to increase the length of the session identification flag. If the length of the session identification flag were that of an integer (on most systems this would be 4 bytes or 32

bits long), the chance for a random match would be 1 in 2^{32} or about 1 in 4 billion.

The security system and the method for embedding a session identifier in the networking protocol disclosed herein have diverse applicability in a range of markets including financial services, horizontal wireless LAN (e.g., wireless sales force automation and contractor services), and government regulated markets such as banking and healthcare. However, these are merely exemplary applications: the present invention is not limited thereto.

Although the present invention has been largely described in terms of providing identification for a user attempting to connect to and communicate a message with a resource/application on a computer system (e.g., and application server), it is not limited thereto. As described herein, for example, the present invention may be embodied in software, in a machine (e.g., a computer system, a microprocessor based appliance, etc.) that includes software in memory, or in a computer readable carrier configured to carry out the protection scheme (e.g., in a self contained silicon device, a solid state memory, an optical disk, a magnetic disk, a radio frequency carrier wave, and audio frequency carrier wave, etc.).

Although the present invention has primarily been described in terms of a message being transmitted between a client and a server, it is not limited to. The identification techniques disclosed herein apply to communications transmitted with respect to a wide range of computer applications, and are not limited to server applications.

The terms message and communication as used herein are intended to refer to a broad class of transmissions carried out between computer systems or portions thereof; for example, inquiries, data updates, data edits, data requests, etc.

Although the invention is illustrated and described herein with reference to specific embodiments, the invention is not intended to be limited to the details shown. Rather, various modifications may be made in the details within the scope and range equivalents of the claims and without departing from the invention.

What is Claimed:

1. A method of identifying the originator of a message transmitted between a client and a server system, said method comprising the steps of:

- modifying a message to be transmitted between a client and a server system to include a session identification flag and a session identifier at an end of the message;

- re-computing a control portion of the message to reflect the inclusion of the session identification flag and the session identifier at the end of the message;

- transmitting the message between the client and the server system;

- checking the transmitted message for the session identification flag;

- reading the session identifier of the transmitted message to determine the originator of the message;

- removing the session identification flag and the session identifier from the transmitted message; and

- re-computing the control portion of the message to reflect the removal of the session identification flag and the session identifier.

2. A computer system comprising;
 - a microprocessor; and
 - a computer readable medium including computer program instructions which cause the computer system to implement a method of identifying the originator of a message transmitted between a client and a server system, said method comprising the steps of:

- modifying a message to be transmitted between a client and a server system to include a session identification flag and a session identifier at an end of the message,

re-computing a control portion of the message to reflect the inclusion of the session identification flag and the session identifier at the end of the message,

transmitting the message between the client and the server system,

checking the transmitted message for the session identification flag,

reading the session identifier of the transmitted message to determine the originator of the message,

removing the session identification flag and the session identifier from the transmitted message, and

re-computing the control portion of the message to reflect the removal of the session identification flag and the session identifier.

3. A computer readable carrier including computer program instructions which cause a computer to implement a method of identifying the originator of a message transmitted between a client and a server system, said method comprising the steps of:

modifying a message to be transmitted between a client and a server system to include a session identification flag and a session identifier at an end of the message,

re-computing a control portion of the message to reflect the inclusion of the session identification flag and the session identifier at the end of the message,

transmitting the message between the client and the server system,

checking the transmitted message for the session identification flag,

reading the session identifier of the transmitted message to determine the originator of the message,

removing the session identification flag and the session identifier from the transmitted message, and

re-computing the control portion of the message to reflect the removal of the session identification flag and the session identifier.

ABSTRACT

A method of identifying the originator of a message transmitted between a client and a server system is provided. The method includes modifying a message to be transmitted between a client and a server system to include a session identification flag and/or a session identifier (e.g., at an end of the message). The method optionally includes one or more of the steps of re-computing a control portion of the message to reflect the inclusion of the session identification flag and the session identifier; transmitting the message between the client and the server system, and checking the transmitted message for the session identification flag; reading the session identifier of the transmitted message to determine the originator of the message; removing the session identification flag and/or the session identifier from the transmitted message; and re-computing the control portion of the message to reflect the removal of the session identification flag and/or the session identifier.

Figure 1

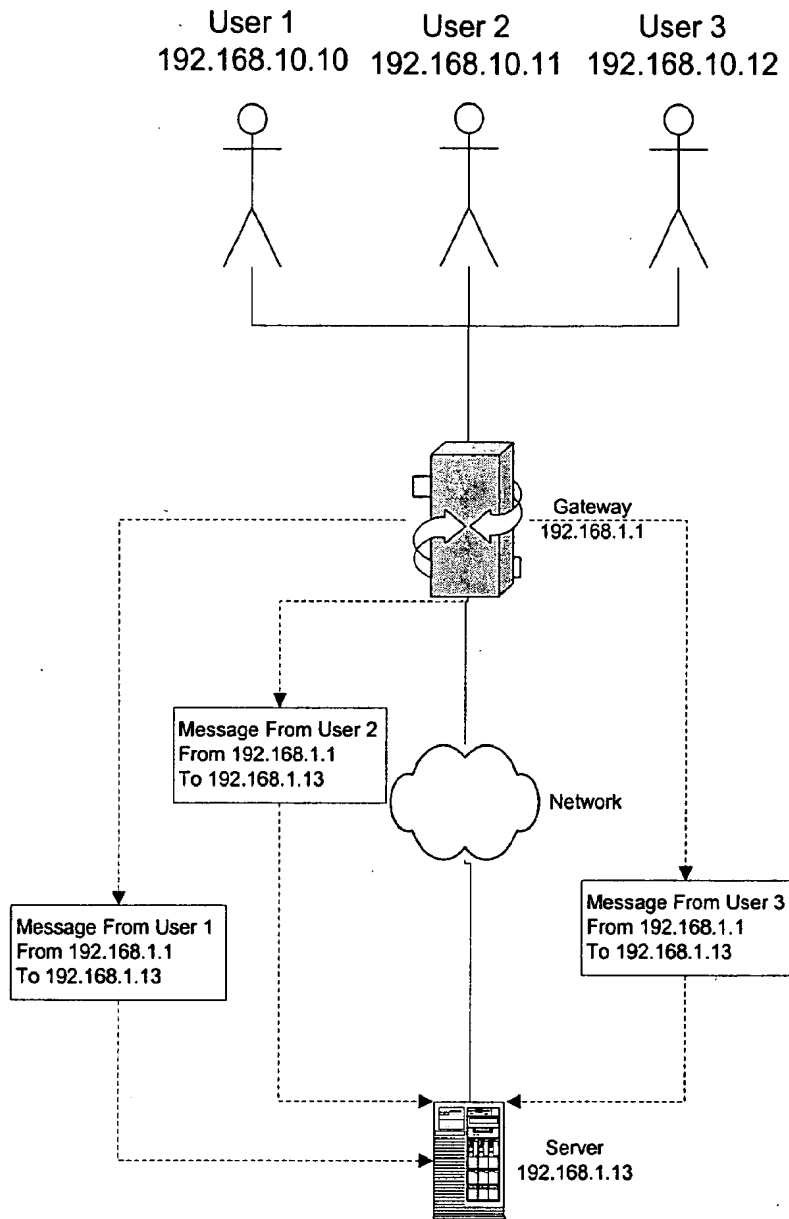


Figure 2

| Control | | Payload |
|---------------------|---------------------------|-------------------------|
| Routing Information | Other Control Information | Data to be communicated |

Figure 3

| Control | | Payload | Flag | Session Identifier |
|------------------------------|---------------------------|-------------------------|------|--------------------|
| Modified Routing Information | Other Control Information | Data to be communicated | | |

Figure 4

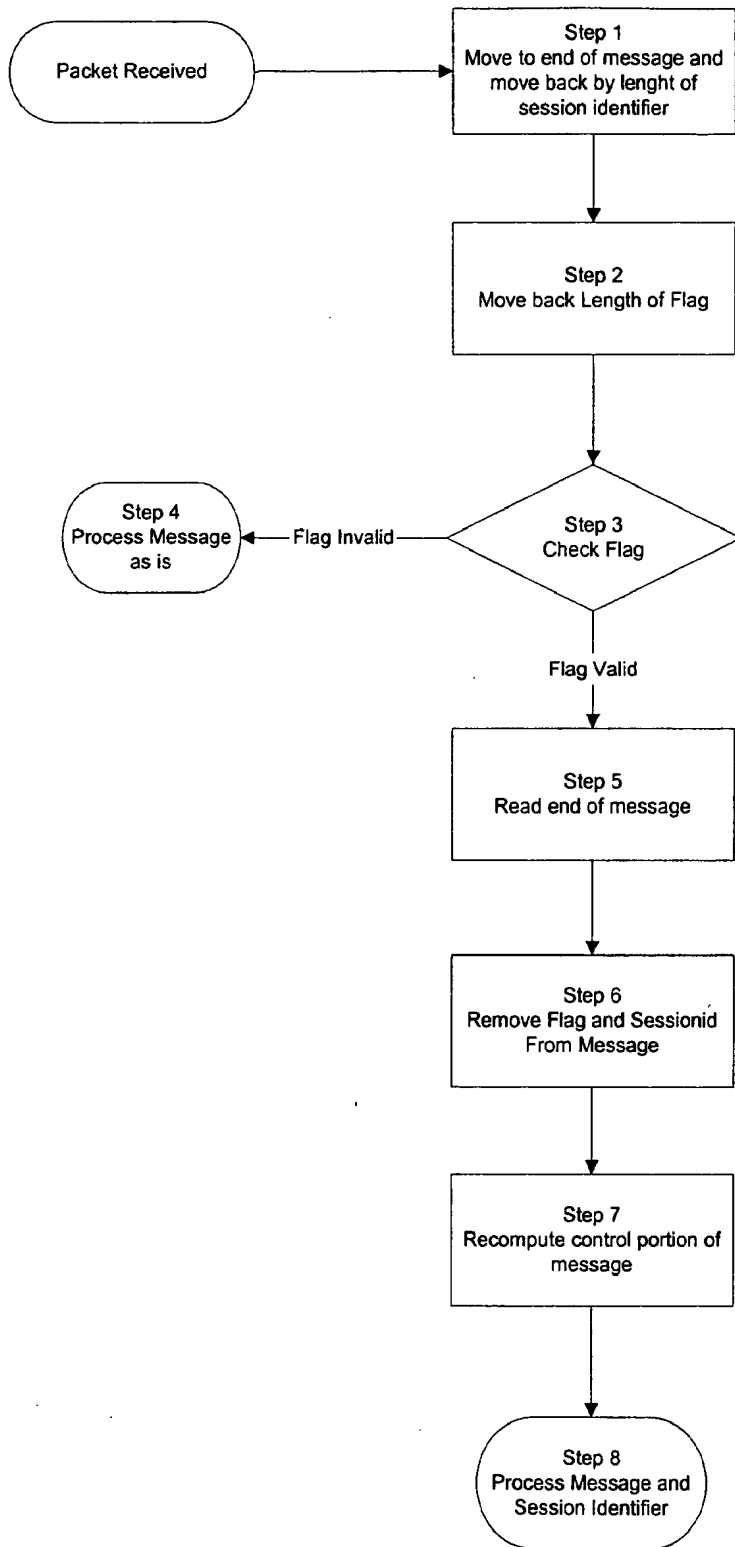


Figure 5

